REMARKS

Applicants provide the present Amendment concurrent with a Request for Continued Examination. Applicants request entry of the amendments herein prior to continued examination.

The § 101 rejections

Applicants have amended independent Claim 45 such that it now recites:

A computer readable medium comprising computer program code embodied therein for monitoring a networked computer system when executed on a computer, the computer program code comprising:
program code configured to sequentially poll a plurality of devices of the networked computer system for data relating to network communications thereof;
program code configured to detect an anomaly responsive to polling of a first device in the computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system; and
program code configured to determine a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites following the detection of the anomaly and prior to polling of the second device.

Dependent Claims 46-52 have been amended in keeping with the amendment to independent Claim 45. Applicants submit that these amendments overcome the rejections of Claims 45-52 under 35 U.S.C. § 101 on pages 2 and 3 of the Final Action.

Claims 29-52 are patentable

Applicants further request reconsideration and withdrawal of the rejections of Claims 29-52 under 35 U.S.C. § 103. In particular, independent Claims 29 and 45 stand rejected as being allegedly obvious with respect to a combination of U.S. Patent Application Publication No. 2003/0110392 to Aucsmith et al. ("Aucsmith") and U.S. Patent Application Publication No. 2002/0078382 to Sheikh et al. ("Sheikh"). Final Action, p. 3. The Final Action asserts that Aucsmith discloses all of the recitations of Claim 29 except "polling a plurality of devices of the networked computer system," but asserts that Sheik teaches "polling a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communication thereof [Fig. 1, 1A, paragraph 0032 lines 5-9,

0042, Fig. 4]" and that it would have been obvious to combine Aucsmith and Sheikh "since one would have been motivated to monitor the computer network systems for security purposes [Sheikh, paragraph 003]." Final Action, p. 4.

Applicants note that, because Aucsmith does not teach "polling a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communication thereof," it also follows that Aucsmith does not disclose or suggest "determining a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites *following the detection of the anomaly and prior to polling of the second device*," *i.e.*, Aucsmith does not disclose or suggest the specific timing relationship between anomaly detection responsive to polling of a first device, determination that a second device "is anticipated to be affected by the anomaly" and polling of the second device recited in Claims 29 and 45. While the cited material from Sheikh generically describes polling, it also does not disclose or suggest the timing relationships recited in the claims.

In particular, with respect to polling, the cited passage in paragraph 0032 of Sheikh merely states "the central server 110a provides for polling of one or more agent transports," and includes no indication of any particular relationship regarding a timing relationship between this polling and anomaly detection responsive to polling of a first device or determination that a second device "is anticipated to be affected by the anomaly." The cited paragraph 0042 merely indicates that polling may occur in a "parallel" or "serial" manner, but also lacks any disclosure or suggestion of any particular relationship regarding a timing relationship between this polling and anomaly detection responsive to polling of a first device or determination that a second device "is anticipated to be affected by the anomaly."

In response to these arguments, the Final Action further elaborates on the polling mechanism described in Sheikh, namely, that Sheikh describes a master transport that polls one or more agent transports (which implement sensor programs) to receive information from the agent transports. Final Action, p. 10. However, this description of Sheikh still fails to provide a reasoned basis as to how or why the proposed combination of Aucsmith and Sheikh teaches any particular temporal relationship between the polled information transfer described in Sheikh and anomaly detection as described in Aucsmith, other than a conclusory assertion that "the combination is sufficient to incorporate the teaching of Sheikh into the

teaching of Aucsmith." Final Action, p. 10. Furthermore, contrary to the implication of the Final Action that a "timing relationship" is not "stated expressively in the claim language" (Final Action, p. 10), Claim 29 expressly recites " determining a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites *following* the detection of the anomaly *and prior to* polling of the second device," *i.e.*, Claim 29 recites a specific temporal relationship between anomaly detection and polling (Claim 45 includes corresponding recitations). As noted above, the proposed combination of Aucsmith and Sheikh provides no such teachings. Accordingly, as the cited combination of Aucsmith and Sheikh does not disclose or suggest all of the recitations of Claims 29 and 45 and, for at least these reasons, Applicants submit that Claims 29 and 45 are patentable.

Applicants submit that dependent Claims 31-35, 43, 44 and 46-52 are patentable at least by virtue of the patentability of the respective ones of independent Claims 29 and 45 from which they depend. Applicants further submit that several of the dependent claims are separately patentable.
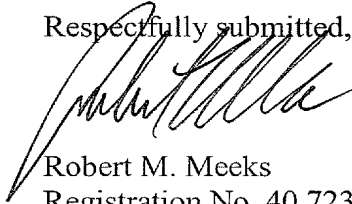
For example, Claim 44 recites "wherein determining a second device that is anticipated to be affected by the anomaly is followed by comprising sending an alert to the second device prior to polling of the second device." Claim 52 includes corresponding computer program product recitations. As discussed above, the cited references, whether taken alone or in combination, do not disclose or suggest specific recited relationships between polling and detection of anomalies and, for at least similar reasons, the cited references also do not disclose or suggest the specific timing relationships between polling and alerts recited in Claims 44 and 52. For at least these reasons, Applicants submit that Claims 44 and 52 are separately patentable.

Conclusion

As all of the claims are in condition for allowance, Applicants respectfully request allowance of the claims and passing of the application to issue in due course. Applicants urge the Examiner to contact Applicants' undersigned representative at (919) 854-1400 to resolve any remaining formal issues.

In re: Jeffrey A. Aaron et al.
Serial No.: 10/811,585
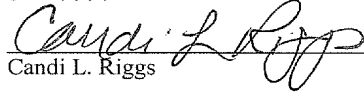Filed: March 29, 2004
Page 9

Respectfully submitted,

Robert M. Meeks
Registration No. 40,723
Attorney for Applicants

USPTO Customer No. 39072
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401

CERTIFICATION OF TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on May 13, 2008.

Candi L. Riggs